The National Strategy for Trusted Identities in Cyberspace: Why We Need It

NSTIC provides a framework for individuals and organizations to utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation.

Shopping, banking, social networking, accessing your employer's intranet – these activities and more are all routinely done online. The increasing availability of these services results in greater opportunities for innovation and economic growth, but the online infrastructure for supporting these services has not evolved at the same pace. The National Strategy for Trusted Identities in Cyberspace addresses two central problems impeding economic growth online:

1. Passwords are inconvenient and insecure
2. Individuals are unable to prove their true identity online for significant transactions

ID Theft and Online Fraud: By the Numbers

Identity theft is costly, inconvenient and all-too common

- In 2010, 8.1 million U.S. adults were the victims of identity theft or fraud, with total costs of $37 billion.[1]
- The average out-of-pocket loss of identity theft in 2008 was $631 per incident.[2]
- Consumers reported spending an average of 59 hours recovering from a “new account” instance of ID theft.[3]

Phishing continues to rise, with attacks becoming more sophisticated

- In 2008 and 2009, specific brands or entities were targeted by more than 286,000 phishing attacks, all attempting to replicate their site and harvest user credentials. [4]
- A 2009 report from Trusteer found that 45% of targets divulge their personal information when redirected to a phishing site, and that financial institutions are subjected to an average of 16 phishing attacks per week, costing them between $2.4 and $9.4 million in losses each year.[5]

Managing multiple passwords is expensive

- A small business of 500 employees spends approximately $110,000 per year on password management. That’s $220 per user per year.[6]

Passwords are failing

- In December 2009, the Rockyou password breach revealed the vulnerability of passwords. Nearly 50% of users’ passwords included names, slang words, dictionary words or were extremely weak, with passwords like “123456”.[7]

Maintenance of multiple accounts is increasing as more services move online

- One federal agency with 44,000 users discovered over 700,000 user accounts, with the average user having 16 individual accounts.[8]

Improving identity practices makes a difference

- Implementation of strong credentials across the Department of Defense resulted in a 46% reduction in intrusions.[9]
- Use of single sign-on technologies can reduce annual sign-in time by 50 hours/user/year.[10]

[1] Javelin Strategy and Research “2011 Identity Fraud Survey Report,” February 2011

[2] Ibid.

[3] Ibid.

[4] Anti-Phishing Working Group. “Global Phishing Survey: Trends and Domain Name Use in 1H2010.” October 2010, accessed April 6, 2011 at http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf.

[5] “Measuring the Effectiveness of In-the-Wild Phishing Attacks.” Trusteer, Inc., December 2, 2009. http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf.

[6] “Are Passwords Really Free? A closer look at the hidden costs of password security.” RSA working paper CLHC WP 204. 2004.

[7] “Consumer Passwords Worst Practices.” The Imperva Application Defense Center (ADC), Imperva, 2010. http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf.

[8] Agency response to internal U.S. Government survey, December 2007.

[9] Lt Gen Charles Croom, Director, DISA and Commander, Joint Task Force-Global Network Operations, 2007.

[10] Gebel, G. “Building the Business Case for Identity Management Investment.” Directory and Security Strategies, Methodologies and Best Practices. *The Burton Group*. 11 August 2004.